

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/002786**A. CLASSIFICATION OF SUBJECT MATTER**
IPC 7 H04L12/66

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHEDMinimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 732 074 A (BRAITBERG MICHAEL F ET AL) 24 March 1998 (1998-03-24) column 1, line 25 - line 35 column 2, line 11 - line 52	1,11
A	US 2003/028612 A1 (LIN RUI ET AL) 6 February 2003 (2003-02-06) page 1, paragraph 7 - paragraph 9 page 3, paragraph 28 - paragraph 29	1,11
A	US 6 519 241 B1 (THEIMER WOLFGANG) 11 February 2003 (2003-02-11) column 1, line 34 - line 44	1,11
A	WO 03/010669 A (NICODEMUS BLAIR GAVOR ; POROZNI BARRY (US); SCHILLE GLENN ALAN (US)) 6 February 2003 (2003-02-06) page 1, line 8 - page 2, line 18	1,11

☐ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *G* document member of the same patent family

Date of the actual completion of the international search

7 April 2005

Date of mailing of the international search report

14/04/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Brichau, G

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No
PCT/FR2004/002786

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5732074	A	24-03-1998	AU 1525197 A	11-08-1997
			CA 2243454 A1	24-07-1997
			EP 1515496 A2	16-03-2005
			EP 0875111 A1	04-11-1998
			WO 9726750 A1	24-07-1997
US 2003028612	A1	06-02-2003	NONE	
US 6519241	B1	11-02-2003	AT 261638 T	15-03-2004
			DE 59810949 D1	15-04-2004
			EP 1445910 A2	11-08-2004
			EP 0918423 A2	26-05-1999
			JP 11275250 A	08-10-1999
			US 2003076792 A1	24-04-2003
WO 03010669	A	06-02-2003	EP 1410212 A1	21-04-2004
			JP 2004537125 T	09-12-2004
			WO 03010669 A1	06-02-2003

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L12/66

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EP0-Internal, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 5 732 074 A (BRAITBERG MICHAEL F ET AL) 24 mars 1998 (1998-03-24) colonne 1, ligne 25 - ligne 35 colonne 2, ligne 11 - ligne 52	1,11
A	US 2003/028612 A1 (LIN RUI ET AL) 6 février 2003 (2003-02-06) page 1, alinéa 7 - alinéa 9 page 3, alinéa 28 - alinéa 29	1,11
A	US 6 519 241 B1 (THEIMER WOLFGANG) 11 février 2003 (2003-02-11) colonne 1, ligne 34 - ligne 44	1,11
A	WO 03/010669 A (NICODEMUS BLAIR GAVOR ; POROZNI BARRY (US); SCHILLE GLENN ALAN (US)) 6 février 2003 (2003-02-06) page 1, ligne 8 - page 2, ligne 18	1,11

☐ Voir la suite du cadre C pour la fin de la liste des documents☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

T document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

X document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

Y document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

Z document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

7 avril 2005

Date d'expédition du présent rapport de recherche internationale

14/04/2005

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentiaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Brichau, G

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5732074	A	24-03-1998	AU 1525197 A	11-08-1997
			CA 2243454 A1	24-07-1997
			EP 1515496 A2	16-03-2005
			EP 0875111 A1	04-11-1998
			WO 9726750 A1	24-07-1997
US 2003028612	A1	06-02-2003	AUCUN	
US 6519241	B1	11-02-2003	AT 261638 T	15-03-2004
			DE 59810949 D1	15-04-2004
			EP 1445910 A2	11-08-2004
			EP 0918423 A2	26-05-1999
			JP 11275250 A	08-10-1999
			US 2003076792 A1	24-04-2003
WO 03010669	A	06-02-2003	EP 1410212 A1	21-04-2004
			JP 2004537125 T	09-12-2004
			WO 03010669 A1	06-02-2003

Procédé et dispositif d'accès à un terminal serveur mobile d'un premier réseau de communication au moyen d'un terminal client d'un autre réseau de communication.

1. Domaine de l'invention

5 Le domaine de l'invention est celui des applications sans fil, ou « wireless applications » en anglais.

Par application sans fil, on entend, selon une définition communément admise, tout type d'applications temps-réel embarquées nécessitant pour communiquer une connexion vers un réseau sans fil et/ou mobile, du type réseau
10 GSM, GPRS, et/ou UMTS par exemple, autres que les applications de téléphonie mobile et « mains libres ».

Plus précisément, l'invention concerne les terminaux mobiles serveurs exécutant de telles applications sans fil destinées à rendre accessibles différents types d'informations et/ou différents types de services auprès d'autres terminaux
15 clients fixes et/ou mobiles distants. Ces différents types de services peuvent être soit spécifiques et ne concerner qu'un ensemble restreint d'individus, soit être génériques et/ou publiques, et être ainsi potentiellement accessibles à tout individu (consultation de pages web sur le réseau Internet, par exemple).

Ainsi, l'invention s'applique notamment, mais non exclusivement, à l'accès
20 par un terminal client fixe ou mobile à un terminal serveur mobile, pour l'utilisation de services et/ou la consultation ou la mise à jour d'informations rendus disponibles par le terminal serveur mobile.

A titre d'exemple illustratif et non limitatif, l'invention s'applique ainsi notamment et non exclusivement à des domaines aussi variés que ceux :

- 25
- l'automotive ;
 - les applications en mode point à point du type M2M (pour « machine to machine » en anglais) ;
 - les applications de télé médecine embarquées sur des terminaux mobiles ;
 - la consultation de pages web mises à disposition par un terminal serveur
30 mobile.

2. L'art antérieur

Aujourd'hui, les terminaux serveurs mobiles, du type téléphones mobiles ou autres terminaux portables de radiocommunication sont de plus en plus utilisés. L'usage de tels terminaux serveurs mobiles est cependant fortement limité par le fait que ces derniers doivent nécessairement être connectés sur un réseau mobile privé et qu'ils ne peuvent donc être accédés que par des terminaux clients fixes ou mobiles également connectés sur le même réseau privé.

En effet, il convient de préciser que tout réseau de communication mobile est fortement sécurisé au moyen d'un ou plusieurs par-feux. De ce fait, il n'est pas possible d'accéder directement à un terminal serveur mobile qui serait connecté sur un tel réseau de communication mobile protégé par ce ou ces par-feux, à partir d'un terminal client fixe ou mobile qui n'appartiendrait pas à ce même réseau mobile.

De façon plus précise et comme illustré sur le figure 1, aucun terminal serveur mobile (10) d'un réseau public terrestre (11) d'un opérateur (PLMN pour « Public Land Mobile Network » en anglais), ne peut être accédé depuis un terminal client (13) d'un autre réseau externe (14), (Internet, par exemple). Ainsi, seul un terminal client appartenant au même réseau public terrestre qu'un terminal serveur mobile pourra accéder et/ou utiliser les services de ce terminal serveur mobile. Trois contraintes techniques principales favorisent cette situation :

- tout d'abord, sur un réseau public terrestre (11) d'un opérateur (PLMN), toute adresse IP (« Internet Protocol » en anglais ou protocole Internet en français) d'identification d'un terminal serveur est allouée dynamiquement. Cette adresse IP dynamique n'existe donc que sur le réseau public terrestre l'ayant allouée. Elle n'est donc connue que des seuls terminaux clients appartenant à ce même réseau public privé, lesquels sont les seuls à pouvoir accéder et/ou utiliser les services dudit terminal serveur mobile ;
- ensuite, sur un réseau public terrestre d'un opérateur (PLMN) est mis en œuvre un mécanisme (15) d'optimisation du nombre des adresses IP utilisées, lequel a pour fonction de traduire chaque port de communication public sollicité sur le réseau en un port de communication privé

uniquement reconnu par ce réseau. Un tel mécanisme (15), plus connu sous le terme anglais NAT (pour « Network Address Translator » ou « Traducteur d'adresses réseau » en français) permet ainsi d'allouer dynamiquement un identifiant privé à chacune des applications exécutées par chacun des terminaux serveurs mobiles d'un même réseau public terrestre ;

- enfin, dans la très grande majorité des cas, la configuration des pare-feux (16) destinés à protéger un réseau public terrestre mobile (11) est réalisée de façon à interdire toute requête entrante (18) du type TCP/IP (pour « Transfert Control Protocol / Internet Protocol » en anglais, ou « protocole de contrôle de transfert / Protocole Internet » en français).

3. Objectifs de l'invention

L'invention a notamment pour objectif de pallier ces inconvénients principaux de l'art antérieur.

Plus précisément, un objectif de l'invention est de fournir une technique permettant de communiquer avec un terminal mobile serveur d'un premier réseau public terrestre (PLMN), depuis un terminal client fixe ou mobile d'un second réseau public terrestre, malgré les contraintes techniques précitées de sécurisation dudit premier réseau.

En d'autres termes, un objectif de l'invention est de fournir une technique permettant d'accéder aux services et/ou aux informations d'un terminal serveur mobile d'un premier réseau public terrestre mobile d'un opérateur, à partir d'un terminal client, fixe ou mobile, n'appartenant pas nécessairement au même premier réseau. Il convient de noter que la formulation de ce problème, qui va également à l'encontre des habitudes de l'homme du métier, fait en soi partie de l'invention.

Un autre objectif de l'invention est de fournir une telle technique qui n'utilise pas les méthodes de connexion habituelles de l'art antérieur essentiellement basées sur des échanges de requêtes TCP/IP pour établir une session de communication avec un terminal serveur mobile, à partir d'un terminal client.

Un autre objectif de l'invention est de fournir une telle technique qui puisse intégrer différents niveaux de sécurisation, d'une part en termes d'initialisation d'une session de communication avec un terminal serveur mobile d'un premier réseau terrestre de communication et d'autre part, en termes d'accès aux services et/ou informations dudit terminal serveur mobile, depuis un autre terminal fixe ou mobile n'appartenant pas au même premier réseau.

Un objectif supplémentaire de l'invention est de fournir une telle technique qui permette également de s'affranchir des contraintes techniques de sécurisation de l'art antérieur précitées pour l'établissement d'une session de communication entre un terminal serveur mobile appartenant à un premier réseau public terrestre (PLMN) et un terminal client appartenant à un autre réseau, mais souhaitant accéder ou utiliser les données et/ou services dudit terminal serveur mobile.

Encore un objectif de l'invention est de fournir une telle technique qui favorise la convergence technique entre les applications sans fil ou mobiles du type M2M et les services Web.

Encore un dernier objectif de l'invention est de fournir une telle technique qui soit simple et peu coûteuse à mettre en œuvre.

4. Caractéristiques principales de l'invention

Ces objectifs, ainsi que d'autres qui apparaîtront par la suite sont atteints à l'aide d'un procédé d'accès d'au moins un terminal client connecté à un premier réseau de communication, aux données et/ou services d'un terminal serveur connecté à un second réseau de communication, les premier et second réseaux pouvant cohabiter ou former un unique réseau. Une des difficultés solutionnées par l'invention réside en particulier dans le fait que le terminal serveur est un terminal serveur mobile. Ainsi, un tel procédé selon l'invention comprend avantageusement au moins les étapes suivantes :

- d'initialisation d'une session de communication par le terminal client avec le terminal serveur mobile ;
- d'établissement de la session de communication par ouverture d'un tunnel de communication direct entre le terminal client et le terminal serveur mobile ;

de façon que ledit terminal client puisse consulter des informations rendues disponibles par le terminal serveur mobile et/ou que le terminal client puisse utiliser et/ou interagir avec toute ou partie des services du terminal serveur mobile.

Avantageusement, le second réseau de communication auquel appartient le
5 terminal serveur mobile est un réseau de communication mobile sans fil accessible au travers d'un par-feu de sécurisation.

Préférentiellement, l'étape d'initialisation de la communication comprend au moins les étapes successives suivantes :

- 10 - étape A : émission d'une première requête du type TCP (pour « Transfert Control Protocol » en anglais, ou « protocole de contrôle de transfert » en français) du terminal client vers un serveur de noms de domaines ;
- étape B : réception par le terminal client d'une réponse à la première requête, laquelle contient au moins un ensemble de paramètres prédéterminés de connexion à un premier serveur mandaté public
15 appartenant au premier réseau de communication ;
- étape C : connexion du terminal client au premier serveur mandaté public, au moyen des paramètres prédéterminés, du type adresse IP et/ou numéro de port de communication ;
- étape D : transmission par le premier serveur mandaté public d'une
20 demande d'initialisation de session de communication vers un second serveur mandaté privé appartenant au second réseau de communication, sous la forme d'un signal de demande d'accès ;
- étape E : émission d'une deuxième requête de connexion du type TCP par le second serveur mandaté privé, sur un port de communication
25 prédéterminé du terminal serveur mobile ;
- étape F : transmission par le terminal serveur mobile d'un acquittement à la deuxième requête de connexion TCP au second serveur mandaté privé ;
- étape G : émission d'une troisième requête de connexion du type TCP par le second serveur mandaté privé sur un port de communication
30 prédéterminé du premier serveur mandaté public ;

- étape H : transmission par le premier serveur mandaté public d'un acquittement à la troisième requête de connexion TCP au second serveur mandaté privé ;
- étape I : transmission par le premier serveur mandaté public d'un acquittement à la première requête de connexion TCP au terminal client.

5 Ainsi, l'enchaînement successif de ces différentes étapes permet avantageusement d'initier une session de communication et d'établir l'ouverture du tunnel de communication direct entre le terminal client et le terminal serveur mobile, le tunnel traversant le ou les par-feux de sécurisation du réseau sur lequel
10 est connecté le terminal serveur mobile.

Préférentiellement, le signal de demande d'accès transmis par le terminal client est du type appartenant au groupe comprenant au moins :

- un message SMS ;
- un courrier électronique ;

15 et comprend une liste de paramètres prédéterminée.

De façon avantageuse, la liste de paramètres prédéterminée comprend au moins des paramètres du type appartenant au groupe comprenant au moins :

- une adresse IP d'identification du premier serveur mandaté public à l'origine du signal de demande d'accès ;
- un numéro de port de communication d'identification complémentaire du premier serveur mandaté public à l'origine du signal de demande d'accès ;
- une clé au moins de sécurisation de l'étape de demande d'initialisation de la communication.

25 Dans un mode de réalisation préférentiel de l'invention, la liste de paramètres prédéterminée comprend en outre avantageusement au moins un paramètre complémentaire correspondant à un numéro d'appel unique du second terminal serveur, lorsque le signal de demande d'accès est du type message SMS, et/ou correspondant au type de protocole de sécurisation dudit tunnel de
30 communication.

Dans une variante du mode de réalisation préférentiel de l'invention, la liste de paramètres prédéterminée comprend en outre au moins un paramètre complémentaire correspondant à une adresse courriel du second terminal serveur, lorsque le signal de demande d'accès est du type message électronique.

- 5 Préférentiellement, la clé de sécurisation est une clé de négociation et/ou de cryptage.

Dans un mode de réalisation préféré de l'invention, le tunnel de communication établi entre le terminal client et le terminal serveur mobile comprend avantageusement des moyens d'authentification du type HTTP.

- 10 Avantageusement, le tunnel de communication établi entre le terminal client et le terminal serveur mobile comprend des moyens sécurisés de transmission de données du type utilisant au moins :

- le protocole IPSEC ;
- le protocole d'encryptage du tunnel de communication.

- 15 L'invention concerne également de façon avantageuse un dispositif de communication et/ou radiocommunication entre au moins un terminal client et au moins un terminal serveur mobile, caractérisé en ce qu'il met en œuvre le procédé précité d'accès d'au moins un terminal client connecté à un premier réseau de communication, aux données et/ou services d'un terminal serveur connecté à un
- 20 second réseau de communication, les premier et second réseaux pouvant cohabiter ou former un unique réseau.

De façon également avantageuse, le procédé selon l'invention est appliqué aux domaines variés appartenant au groupe comprenant au moins :

- des applications sans fil utilisant des services web ;
- 25 - des applications de télé médecine embarquées permettant à un médecin d'accéder régulièrement au téléphone mobile jouant le rôle d'un terminal serveur mobile, de façon à accéder et contrôler les données d'un patient, propriétaire dudit téléphone mobile;
- des applications distribuées interactives du type comprenant au moins :
- 30 o les jeux distribuées ;

- o les applications de travail collaboratif embarquées sur des terminaux mobiles communicants.

5. Liste des figures

D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation préférentiel, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

- la figure 1 est une illustration de la situation actuelle ou de l'art antérieur concernant l'impossibilité pour un terminal client (fixe ou mobile) connecté à l'Internet, de pouvoir accéder à un terminal serveur mobile d'un réseau public terrestre du type PLMN (pour « Public Land Mobile Network » en anglais) protégé par au moins un par-feu et au moins un traducteur d'adresses réseau publiques en adresses réseau privées (NAT pour « Network Address Translator » en anglais). Cette figure est décrite de façon détaillé au paragraphe 2 : Art antérieur du présent document ;
- la figure 2 illustre les différents composants techniques et les différentes étapes d'initialisation d'une session de communication intervenant respectivement dans le dispositif et le procédé selon l'invention ;
- la figure 3 est un diagramme de séquences explicitant les différentes étapes d'initialisation d'une session de communication conduisant à l'ouverture d'un tunnel de communication entre un terminal client d'un premier réseau de communication et un terminal serveur mobile d'un autre réseau de communication ;
- la figure 4 illustre le schéma de communication entre un terminal client d'un premier réseau de communication et un terminal serveur mobile appartenant à un deuxième réseau privé sécurisé, suite à l'initialisation d'une session de communication et à l'ouverture d'un tunnel de communication traversant le par-feu et le traducteur d'adresse dudit réseau privé, au moyen du procédé selon l'invention.

Les figures 2 à 4 sont décrites de façon détaillées dans la description d'un mode de réalisation préférentielle de l'invention.

6. Rappel du principe général de l'invention

L'invention vise donc à fournir un procédé d'accès aux services ou données d'un terminal serveur mobile d'un réseau public terrestre au moyen d'un terminal client (fixe ou mobile) connecté su un autre réseau de communication, l'Internet par exemple. Un tel procédé s'appuie en particulier sur l'utilisation d'un message du type SMS (pour « Short Message Service » en anglais ou service de message court en français) ou d'un message électronique par le terminal client, pour demander l'initialisation d'une session de communication avec ledit terminal serveur mobile. L'initialisation d'une telle session se traduit en particulier par l'établissement d'un tunnel de communication entre le terminal client et le terminal serveur mobile, lequel traverse de façon sécurisée le par-feu (« firewall » en anglais) et le traducteur d'adresses réseau (NAT pour « Network Address Translator » en anglais)).

Différents modes de réalisation de l'invention sont techniquement envisageables, un d'entre eux étant décrit de façon plus détaillé ci-dessous.

7. Présentation d'un mode de réalisation préférentiel de l'invention

Dans un mode de réalisation préférentielle de l'invention, la solution technique selon l'invention s'appuie sur une démarche originale permettant d'autoriser, moyennant sécurisation, l'initialisation d'une session de communication entre un terminal serveur mobile d'un réseau public terrestre (PLMN) et un terminal client d'un autre réseau, comme si le terminal client appartenait audit réseau public terrestre.

Cette démarche s'appuie notamment sur une utilisation pertinente et originale des messages SMS (pour « Short Message Service » en anglais) comprenant un ensemble de paramètres, pour transmettre directement au serveur mandaté dudit réseau public terrestre une demande d'initialisation de communication avec un terminal serveur mobile préalablement identifié, ce qui permet ainsi de s'affranchir du problème selon l'art antérieur lié à la transmission d'une requête TCP/IP. En effet, toute requête de ce type de demande d'initialisation d'une session de communication avec un terminal serveur mobile d'un PLMN serait

dans tous les cas est bloquée par le par-feu et le traducteur d'adresses réseau de ce PLMN.

De façon avantageuse, le procédé selon l'invention concerne d'une part l'initialisation d'une session de communication par le terminal client avec le terminal serveur mobile, et d'autre part, l'établissement d'une session de communication par ouverture d'un tunnel de communication direct entre le terminal client et le terminal serveur. L'ouverture d'un tel tunnel direct permet ainsi au terminal client de pouvoir consulter des informations rendues disponibles par le terminal serveur et/ou de pouvoir utiliser et interagir avec toute ou partie des services du terminal serveur.

Comme illustré sur les figures 2 et 3, l'étape d'initialisation de la communication comprend au moins les étapes successives suivantes :

- étape A : émission d'une première requête (20, 30) du type TCP (pour « Transfert Control Protocol » en anglais, ou « protocole de contrôle de transfert » en français) du terminal client (200, 300) vers un serveur (201, 301) de noms de domaines ;
- étape B : réception par le terminal client (200, 300) d'une réponse (21, 31) à la première requête (20, 30), laquelle contient au moins un ensemble de paramètres prédéterminés de connexion à un premier serveur mandaté public (202, 302) appartenant au premier réseau de communication (210);
- étape C : connexion (22, 32) du terminal client (200, 300) au premier serveur mandaté public (202, 302), au moyen des paramètres prédéterminés, du type adresse IP et/ou numéro de port de communication;
- étape D : transmission par le premier serveur mandaté public (202, 302) d'une demande (23, 33) d'initialisation de session de communication vers un second serveur mandaté privé (203, 303) appartenant au second réseau de communication (211), sous la forme d'un signal de demande d'accès ;
- étape E : émission d'une deuxième requête (24, 34) de connexion du type TCP par le second serveur mandaté privé (203, 204), sur un port de communication (35) prédéterminé du terminal serveur mobile (204, 304) ;

- étape F : transmission par le terminal serveur mobile (204, 304) d'un acquittement (35) à la deuxième requête (24, 34) de connexion TCP, au second serveur mandaté privé (203, 303) ;
- 5 - étape G : émission d'une troisième requête (36) de connexion du type TCP par le second serveur mandaté privé (203, 303) sur un port de communication (305) prédéterminé du premier serveur mandaté public (202, 302) ;
- étape H : transmission par le premier serveur mandaté public (202, 302) d'un acquittement (37) à la troisième requête de connexion TCP (36), au
10 second serveur mandaté privé (203, 303) ;
- étape I : transmission par le premier serveur mandaté public (202, 302) d'un acquittement (38) à la première requête de connexion TCP (20, 30), au terminal client (200, 300).

Ainsi, comme illustré sur la figure 4, l'enchaînement successif de ces
15 différentes étapes permet d'initier une session de communication et d'établir l'ouverture d'un tunnel de communication direct (40) entre le terminal client (41) et le terminal serveur mobile (42). Grâce au procédé selon l'invention, le tunnel de communication (40) ainsi ouvert traverse le ou les par-feux (43) et traducteurs d'adresses réseau (44) de sécurisation du réseau PLMN privé (45) sur lequel est
20 connecté le terminal serveur mobile (42). Le terminal client (41) est alors en mesure de communiquer directement, en mode point à point (46) avec le terminal serveur mobile (42) et d'utiliser les services ou données rendus disponibles par ce dernier.

Il est bien entendu que sur la figure 3, les ports de communication référencés (35) et (305) sur la figure 3 sont donnés à titre de simple exemple indicatif et non
25 limitatif, d'autres numéros de port de communication pouvant être utilisés, indifféremment en fonction des configurations réseau rencontrées.

Un tel procédé selon l'invention permet ainsi à tout terminal client d'un réseau de communication, du type Internet par exemple, de se connecter à un
30 terminal client mobile d'un réseau public terrestre du type PLMN, comme s'il appartenait lui-même à ce réseau public terrestre sécurisé par des par-feux et

traducteurs d'adresses réseau du type NAT (pour « Network Address Translator » en anglais).

En outre, il est important de souligner que les étapes successives d'initialisation d'une session de communication peuvent être sécurisée par des
5 moyens de cryptage à une ou plusieurs clés publiques et privées. En effet, il est techniquement possible d'envisager l'encapsulation et le cryptage des paramètres prédéterminés contenu dans le message SMS permettant d'établir l'ouverture d'une session de communication et du tunnel de communication associé.

Dans une variante du mode de réalisation préférentielle précité, il est prévu
10 que le terminal client ne transmette pas directement un SMS vers le serveur mandaté privé du réseau public terrestre PLMN, mais transmette à ce serveur mandaté privé un message électronique ou courriel sécurisé par des moyens de cryptage, lequel contient au minimum les mêmes informations de demande d'établissement de la session de communication que celles contenues dans le
15 message SMS du mode de réalisation préférentielle précité :

- une adresse IP d'identification du premier serveur mandaté public à l'origine du signal de demande d'accès ;
- un numéro de port de communication d'identification complémentaire du
20 premier serveur mandaté public à l'origine du signal de demande d'accès ;
- une clé au moins de sécurisation de l'étape de demande d'initialisation de la communication.

Dans les deux modes de réalisation de l'invention précités, la liste de paramètres prédéterminée comprend en outre au moins un paramètre
25 complémentaire correspondant à un numéro d'appel unique du second terminal serveur, lorsque le signal de demande d'accès est du type message SMS, et/ou correspondant au type de protocole de sécurisation dudit tunnel de communication.

8. Avantages de la solution selon l'invention

30 Les procédé et dispositif d'accès d'au moins un terminal client connecté à un premier réseau de communication, aux données et/ou services d'un terminal

serveur mobile connecté à un second réseau de communication fortement sécurisé, tels que proposés par l'invention présentent de nombreux avantages, dont une liste non exhaustive est donnée ci-dessous :

- 5 - amélioration de la convergence entre les applications en mode point à point plus connues sous l'acronyme M2M (pour « Machine To Machine » en anglais) et les applications de l'Internet et/ou les services Web ;
- 10 - possibilité d'embarquer sur des serveurs mobiles de nouvelles applications sans fil ou de nouveaux services à forte valeur ajoutés. De telles applications peuvent notamment concerner à titre d'exemple illustratif et non limitatif, la télé médecine. En effet, l'invention permet d'envisager de nouvelles applications de télé médecine qui permettraient, par exemple, à un patient diabétique, de renseigner directement son taux de glycémie sur son téléphone mobile, son médecin n'ayant plus qu'à
- 15 venir interroger de façon sécurisée les données de sa patiente directement sur le téléphone mobile de cette dernière, lequel jouant le rôle d'un terminal serveur mobile.

REVENDICATIONS

1. Procédé d'accès d'au moins un terminal client connecté à un premier réseau de communication, aux données et/ou services d'un terminal serveur connecté à un second réseau de communication, lesdits premier et second réseaux
5 pouvant cohabiter ou former un unique réseau, caractérisé en ce que ledit terminal serveur est un terminal mobile, et en ce que ledit procédé comprend au moins les étapes suivantes :
- d'initialisation d'une session de communication par ledit terminal client avec ledit terminal serveur mobile ;
 - 10 - d'établissement de ladite session de communication par ouverture d'un tunnel de communication direct entre ledit terminal client et ledit terminal serveur ;
- de façon que ledit terminal client puisse consulter des informations rendues disponibles par ledit terminal serveur et/ou que ledit terminal client puisse utiliser
15 et/ou interagir avec toute ou partie des services dudit terminal serveur.
2. Procédé d'accès d'au moins un terminal client connecté à un premier réseau de communication, aux données et/ou services d'un terminal serveur connecté à un second réseau de communication, selon la revendication 1, caractérisé en ce que ledit second réseau de communication est un réseau de
20 communication mobile sans fil accessible au travers d'un par-feu de sécurisation.
3. Procédé d'accès d'au moins un terminal client connecté à un premier réseau de communication, aux données et/ou services d'un terminal serveur connecté à un second réseau de communication, selon l'une quelconques des revendications 1 et 2, caractérisé en ce que ladite étape d'initialisation de la
25 communication comprend au moins les étapes successives suivantes :
- étape A : émission d'une première requête du type TCP (pour « Transfert Control Protocol » en anglais, ou « protocole de contrôle de transfert » en français) dudit terminal client vers un serveur de noms de domaines ;
 - étape B : réception par le terminal client d'une réponse à ladite première
30 requête, laquelle contient au moins un ensemble de paramètres

- prédéterminés de connexion à un premier serveur mandaté public appartenant audit premier réseau de communication ;
- étape C : connexion dudit terminal client audit premier serveur mandaté public, au moyen desdits paramètres prédéterminés, du type adresse IP et/ou numéro de port de communication ;
 - étape D : transmission par ledit premier serveur mandaté public d'une demande d'initialisation de session de communication vers un second serveur mandaté privé appartenant audit second réseau de communication, sous la forme d'un signal de demande d'accès ;
 - étape E : émission d'une deuxième requête de connexion du type TCP par ledit second serveur mandaté privé, sur un port de communication prédéterminé dudit terminal serveur mobile ;
 - étape F : transmission par ledit terminal serveur mobile d'un acquittement à ladite deuxième requête de connexion TCP au dit second serveur mandaté privé ;
 - étape G : émission d'une troisième requête de connexion du type TCP par ledit second serveur mandaté privé sur un port de communication prédéterminé dudit premier serveur mandaté public ;
 - étape H : transmission par ledit premier serveur mandaté public d'un acquittement à ladite troisième requête de connexion TCP au dit second serveur mandaté privé ;
 - étape I : transmission par ledit premier serveur mandaté public d'un acquittement à ladite première requête de connexion TCP au dit terminal client ;
- de façon à initier ladite session de communication et établir l'ouverture dudit tunnel de communication direct entre le terminal client et le terminal serveur mobile, ledit tunnel traversant ledit par-feu de sécurisation.
4. Procédé d'accès d'au moins un terminal client connecté à un premier réseau de communication, aux données et/ou services d'un terminal serveur connecté à un second réseau de communication, selon la revendication 3,

caractérisé en ce que ledit signal de demande d'accès transmis par ledit terminal client est du type appartenant au groupe comprenant au moins :

- un message SMS ;
- un courrier électronique ;

5 et en ce qu'il comprend une liste de paramètres prédéterminée.

5. Procédé d'accès d'au moins un terminal client connecté à un premier réseau de communication, aux données et/ou services d'un terminal serveur connecté à un second réseau de communication, selon la revendication 4, caractérisé en ce que ladite liste de paramètres prédéterminée comprend au moins
10 des paramètres du type appartenant au groupe comprenant au moins :

- une adresse IP d'identification dudit premier serveur mandaté public à l'origine dudit signal de demande d'accès ;
- un numéro de port de communication d'identification complémentaire dudit premier serveur mandaté public à l'origine
15 dudit signal de demande d'accès ;
- une clé au moins de sécurisation de ladite étape de demande d'initialisation de la communication.

6. Procédé d'accès d'au moins un terminal client connecté à un premier réseau de communication, aux données et/ou services d'un terminal serveur
20 connecté à un second réseau de communication, selon l'une quelconque des revendications 4 et 5, caractérisé en ce que ladite liste de paramètres prédéterminée comprend en outre au moins un paramètre complémentaire correspondant à un numéro d'appel unique dudit second terminal serveur, lorsque ledit signal de demande d'accès est du type message SMS, et/ou correspondant au type de
25 protocole de sécurisation dudit tunnel de communication.

7. Procédé d'accès d'au moins un terminal client connecté à un premier réseau de communication, aux données et/ou services d'un terminal serveur connecté à un second réseau de communication, selon l'une quelconque des revendications 4 et 5, caractérisé en ce que ladite liste de paramètres prédéterminée
30 comprend en outre au moins un paramètre complémentaire correspondant à une

adresse courriel dudit second terminal serveur, lorsque ledit signal de demande d'accès est du type message électronique.

5 8. Procédé d'accès d'au moins un terminal client connecté à un premier réseau de communication, aux données et/ou services d'un terminal serveur connecté à un second réseau de communication, selon la revendication 5, caractérisé en ce que ladite clé de sécurisation est une clé de négociation et/ou de cryptage.

10 9. Procédé d'accès d'au moins un terminal client connecté à un premier réseau de communication, aux données et/ou services d'un terminal serveur connecté à un second réseau de communication, selon l'une quelconque des revendications 1 à 8, caractérisé en ce que ledit tunnel de communication établi entre ledit terminal client et ledit terminal serveur mobile comprend des moyens d'authentification du type HTTP.

15 10. Procédé d'accès d'au moins un terminal client connecté à un premier réseau de communication, aux données et/ou services d'un terminal serveur connecté à un second réseau de communication, selon l'une quelconque des revendications 1 à 9, caractérisé en ce que ledit tunnel de communication établi entre ledit terminal client et ledit terminal serveur mobile comprend des moyens sécurisés de transmission de données du type utilisant au moins :

- 20
- le protocole IPSEC ;
 - le protocole d'encryptage du tunnel de communication.

11. Dispositif de communication et/ou radiocommunication entre au moins un terminal client et au moins un terminal serveur mobile, caractérisé en ce qu'il met en œuvre le procédé selon les revendications 1 à 10.

25 12. Application du procédé selon les revendications 1 à 10 aux domaines appartenant au groupe comprenant au moins :

- des applications sans fil utilisant des services web ;
 - des applications de télé médecine embarquées permettant à un médecin d'accéder régulièrement au téléphone mobile jouant le
- 30 rôle d'un terminal serveur mobile, de façon à accéder et contrôler les données d'un patient, propriétaire dudit téléphone mobile ;

- des applications distribuées interactives du type comprenant au moins :

- les jeux distribuées ;
- les applications de travail collaboratif embarquées sur des terminaux mobiles communicants.

1/4

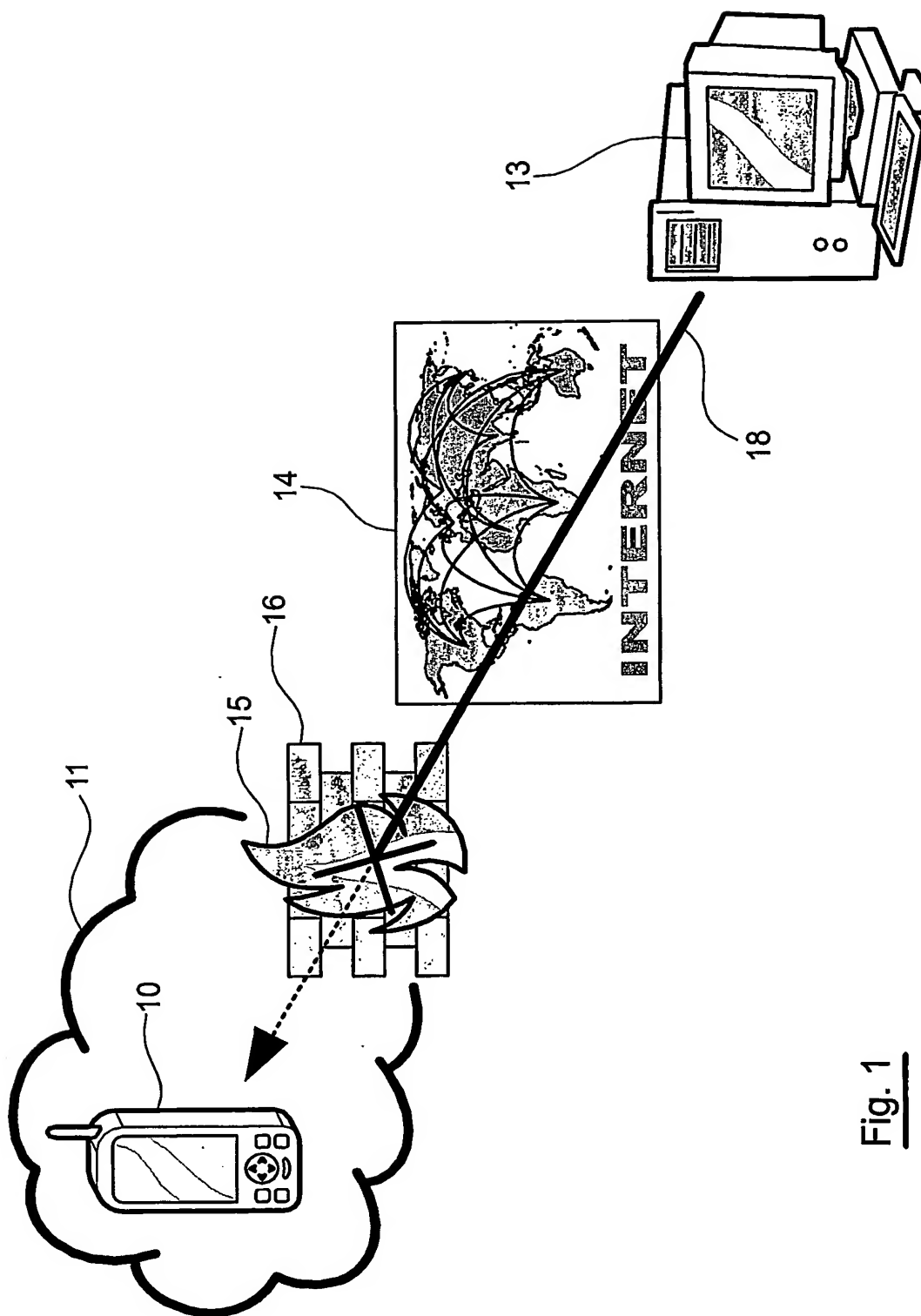


Fig. 1

2/4

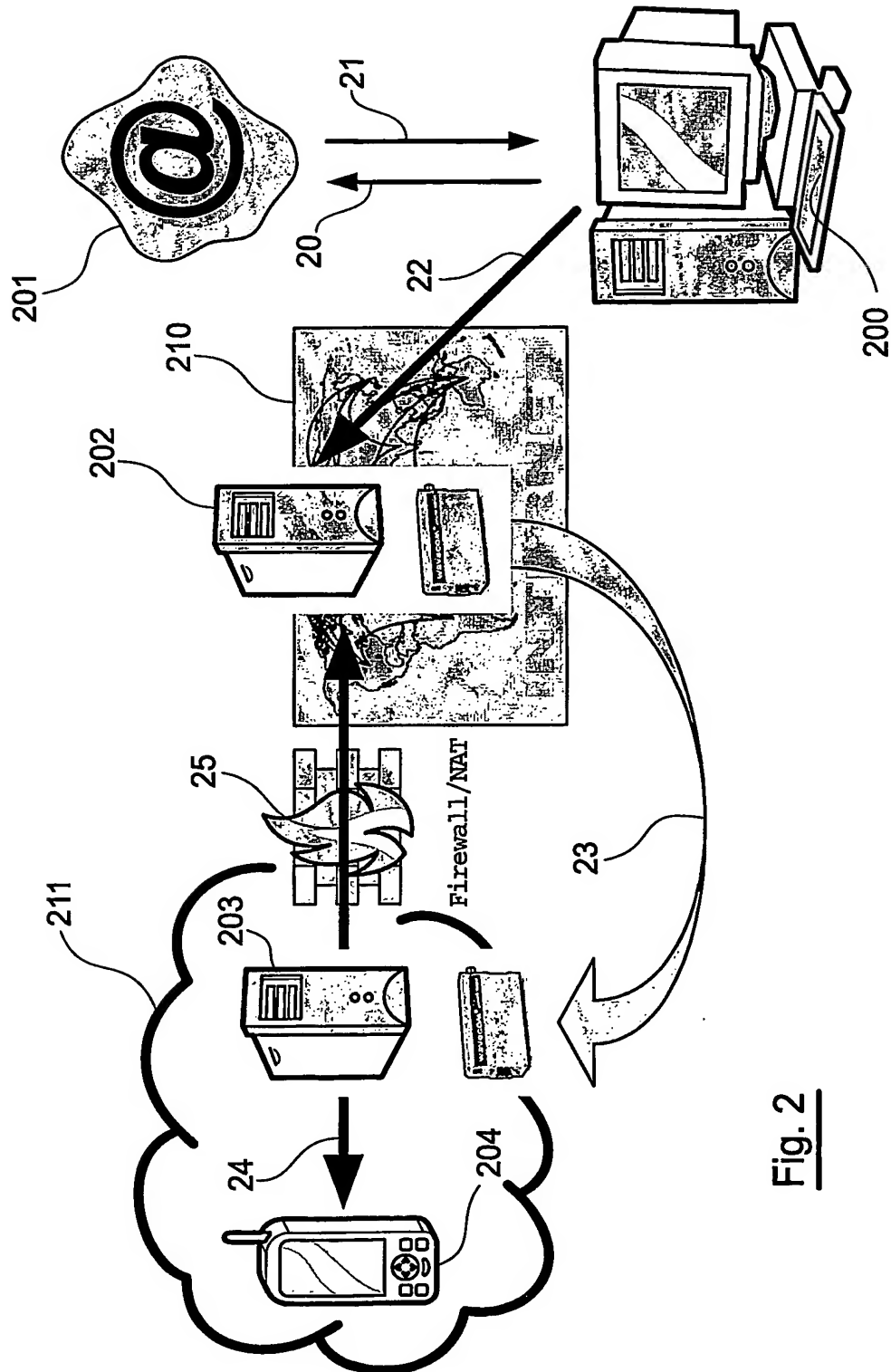


Fig. 2

3/4

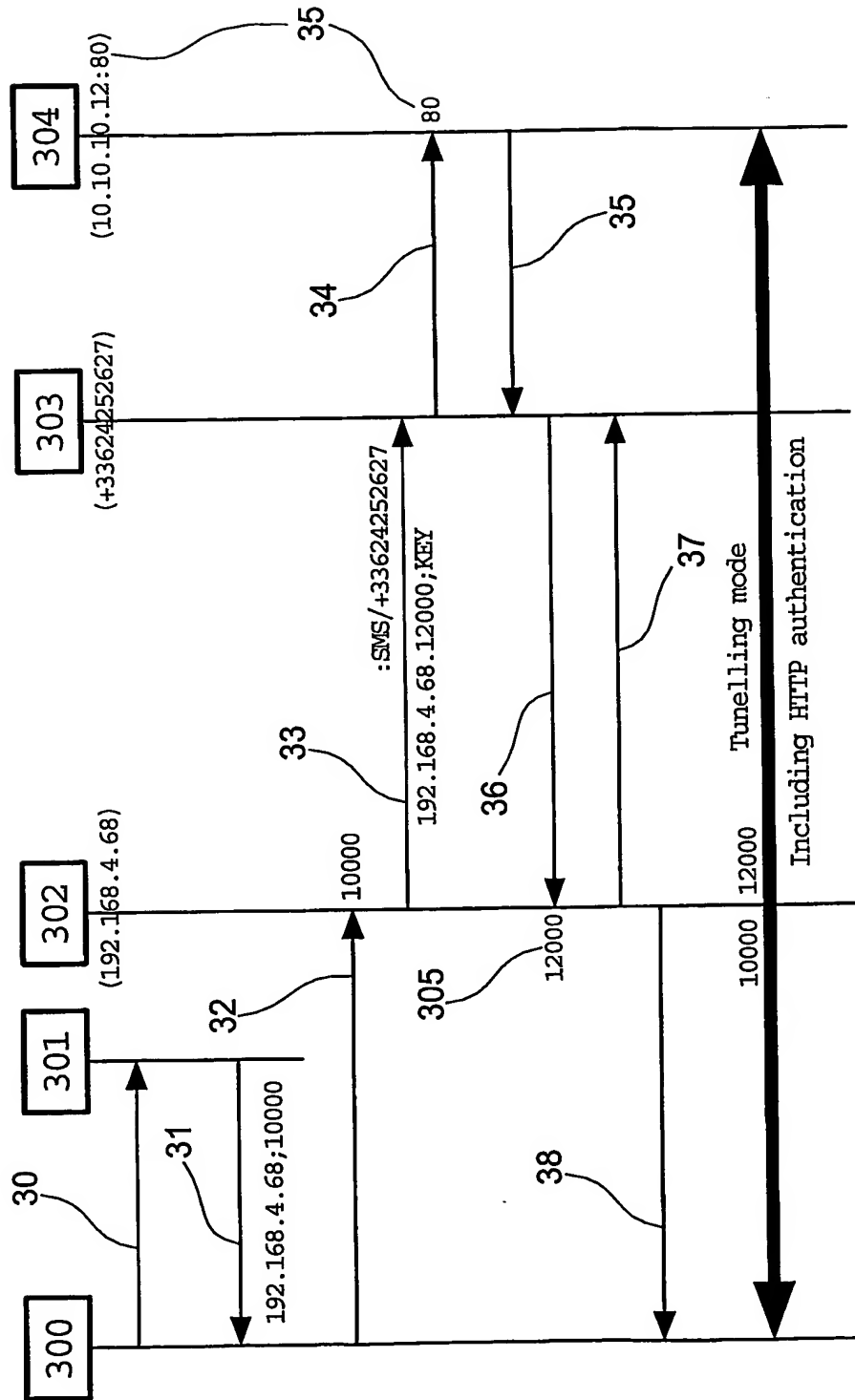


Fig. 3

4/4

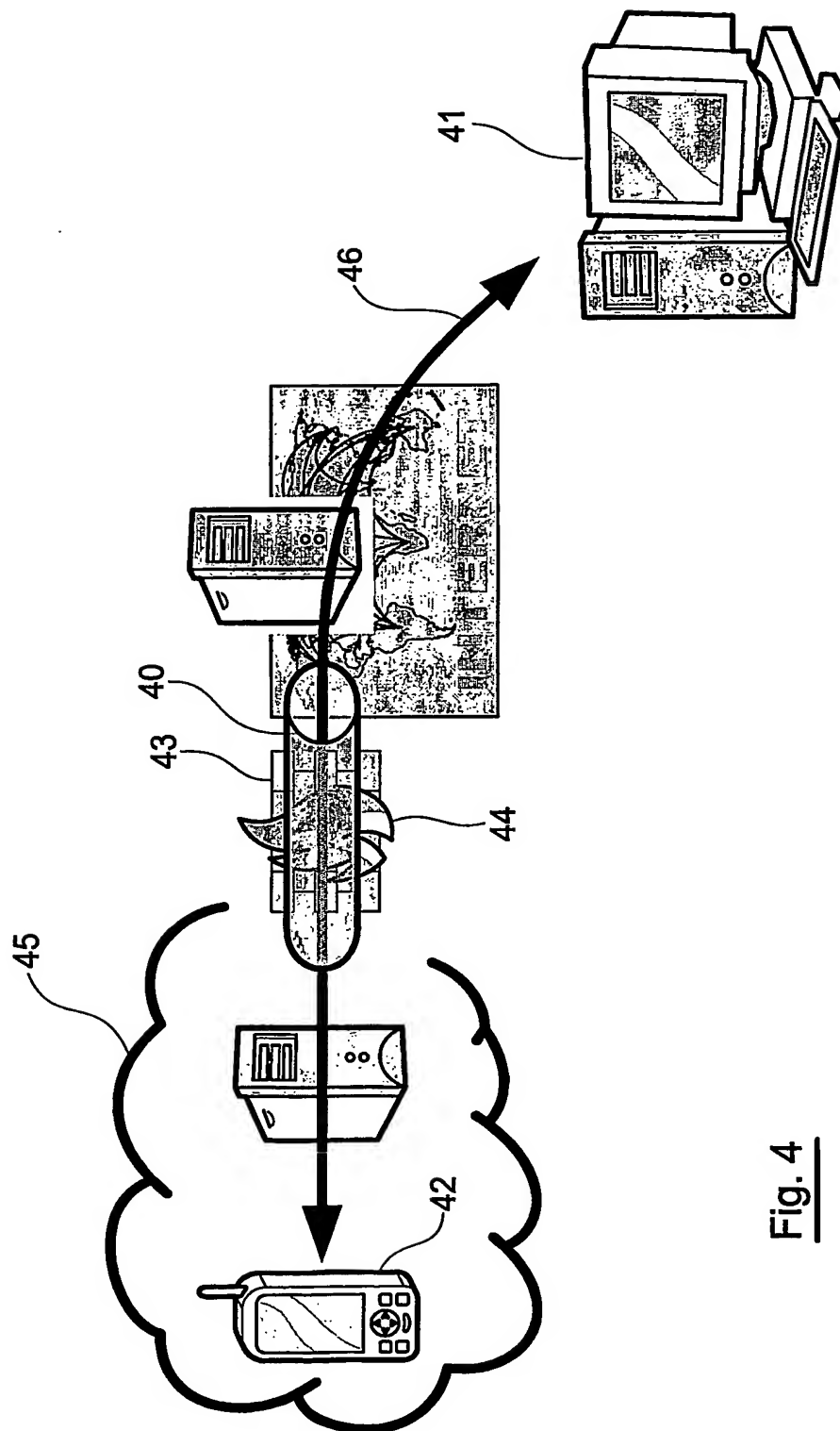


Fig. 4